CORRECTED VERSION*

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : G06F 1/00

A1

(11) International Publication Number: WO 00/08543

(43) International Publication Date: 17 February 2000 (17.02.00)

(21) International Application Number: PCT/US99/17575

(22) International Filing Date: 4 August 1999 (04.08.99)

(30) Priority Data:
09/129,626 5 August 1998 (05.08.98) US

(71) Applicant: SUN MICROSYSTEMS, INC. [US/US]; 901 San Antonio Road, M/S PAL01-521, Palo Alto, CA 94304 (US).

(72) Inventor: TOWNSEND, Timothy, J.; 10590 Chardonnay Lane, Los Altos, CA 94024 (US).

(74) Agents: GARRETT, Arthur, S.; Finnegan, Henderson, Farabow, Garrett & Dunner, L.L.P., 1300 I Street, N.W., Washington, DC 20005-3315 (US) et al.

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published

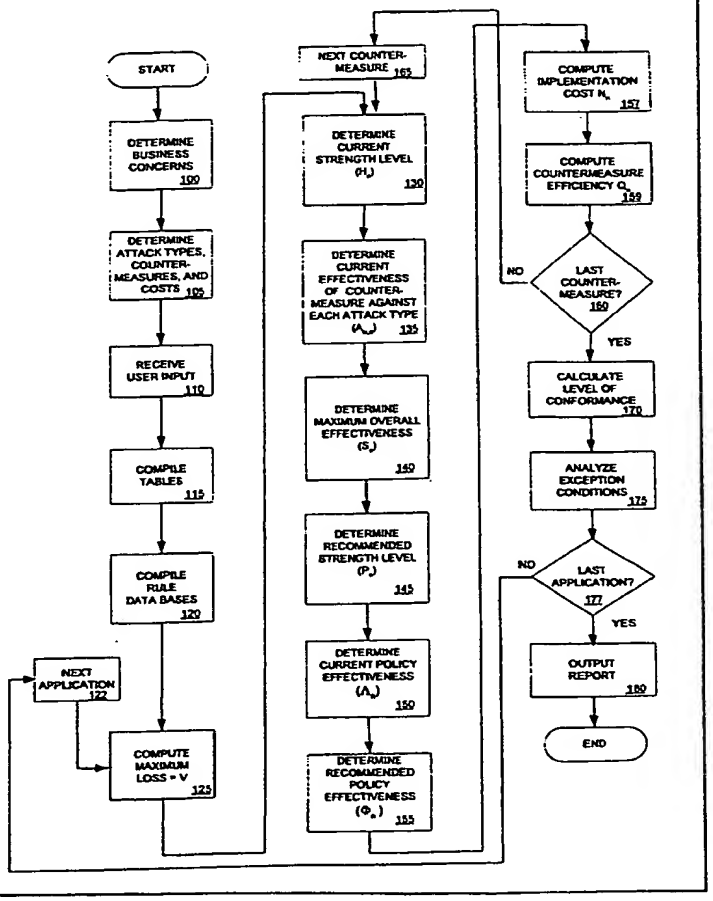
With international search report.

Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: ADAPTIVE COUNTERMEASURE SELECTION METHOD AND APPARATUS

(57) Abstract

A method of selecting a security model for an organization operating an application on the organization's computer network is described. A current strength level for a countermeasure is determined based on input data and rules corresponding to the application. The method and apparatus determine a recommended strength level for countermeasures based on the input data and security risk data. Based on the current strength level and the recommended strength level, the method determines and outputs a security model including a countermeasure and corresponding strength level. The method may also modify the model based on exception conditions. The method may be used to calculate the risk of attack to the application and degree to which the organization conforms to industry practices.



*(Referred to in PCT Gazette No. 31/2000, Section II)

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

ADAPTIVE COUNTERMEASURE SELECTION METHOD AND APPARATUS

BACKGROUND OF THE INVENTION

A. Field of the Invention

This invention relates generally to information security and, more particularly, to improved methods and apparatus for selecting information security solutions based on a multitude of parameters.

B. Description of the Related Art

The number of entities using the Internet and the World Wide Web for all types of business solutions is growing rapidly. At the same time, the need for increased internal security around corporate information systems is also increasing due, in part, to the increased penetration of information systems. Increasing physical security is often not the only solution especially if the business allows access not just to employees, but to personnel outside the organization such as vendors, contractors, and temporary employees.

One common solution to information security risks is to protect information using firewalls. A firewall is a combination of hardware and software that limits the exposure of a computer or group of computers to attacks from the outside. Firewalls provide a single point of entry to protect network resources from unauthorized access. A firewall may comprise, for example, application proxies, access control lists, logging capabilities, or filtering. Relying solely on firewall perimeter protection is often inadequate. Furthermore, firewalls frequently hinder business plans to communicate electronically between customers, suppliers, and business partners.

Other existing security countermeasures include password protection, encryption, and fireridges. A fireridge is essentially a limited firewall operating on an internal network, such as an intranet, and can contain filters, application proxies, and other means for shielding computers from other computers on the internal network. Each of these security countermeasures used alone may be inefficient in part because they were not designed for use with corporate networks or because security holes exist in the overall systems implementation.

Evaluating an organization's overall system of security measures on an application by application basis is very expensive and often difficult. Interpretation of the results of a security risk assessment is often unreliable and subjective because they are conducted by human auditors who may have varying degrees of expertise in systems security engineering and may unknowingly focus on one area of the system more than another. Additionally, conventional risk assessments are often expressed in terms of estimated loss calculated without using formulas or historical data. Consequently, entities in the business of managing risk exposure, such as corporate management or insurance service groups, have few actual tools to use in estimating loss. Furthermore, conventional risk assessment tools, such as annual loss expectancy, do not assist organizations in selecting a less risky security model.

The security of large corporate networks is particularly challenging to assess for many reasons. The networks may have hundreds of different applications systems and servers, thousands of user accounts, and exchange billions of bytes of information with the Internet every day. The sheer volume of users and transactions make it more difficult to design and monitor a secure architecture. The process of inventorying an organization's application systems, the current level of security measures implemented by the organization, and even the applications architecture can be a daunting task. Moreover, once this information is collected, the information is difficult to keep current with the dynamism of the corporation is a difficult task. Without automation, therefore, the task of risk analysis can be further complex and very time consuming to do well.

Therefore, a need exists for an improved method of assessing the information security of large corporate systems in a manner that is based on best industry practices and principles and is reliable, repeatable, cost efficient, and consistent from system to system. Furthermore, a need exists for a method of selecting a security model based on the assessment.

SUMMARY OF THE INVENTION

In accordance with the invention, systems and methods consistent with the present invention create a security model for an organization operating an application on a computer network to protect the application from attack by unauthorized sources.

A current countermeasure strength level and a recommended countermeasure strength level are determined for each of at least one countermeasure based on input data and security risk data. A security model including at least one countermeasure and a corresponding strength level is determined based on the current and the recommended strength levels.

BRIEF DESCRIPTION OF THE DRAWINGS

The accompanying drawings, which are incorporated in and constitute a part of this specification, illustrate an embodiment of the invention and, together with the description, serve to explain the advantages and principles of the invention. In the drawings,

Fig. 1 is a flow diagram representing states of a method consistent with the present invention.

Fig. 2 is an example of a questionnaire consistent with the present invention;

Figs. 3a and 3b are tables showing parameters consistent with the present invention;

Fig. 4 is an example of a data base of rules consistent with the present invention;

Fig. 5 is an example of rules for handling exception conditions consistent with the present invention;

Fig. 6 shows an example of information security policies consistent with the present invention; and

Fig. 7 shows a block diagram of a system consistent with the present invention.

DETAILED DESCRIPTION

Reference will now be made in detail to an implementation consistent with the principles of the present invention as illustrated in the accompanying drawings. Wherever possible, the same reference numbers will be used throughout the drawings and the following description to refer to the same or like parts.

A. Method of Operation

Figure 1 is a flowchart showing states of a method consistent with the present invention. Some aspects of the following method will vary depending on the nature of the activities of an organization being evaluated. The following example describes an organization whose principle activity is the manufacture and development of computer systems.

Consistent with the present invention, the organization begins by determining the business concerns of the organization (state 100). The set C of business concerns include specific consequences against which an organization would like to protect its application assets including, for example, loss of market share, system outage or unavailability, loss of property, and damage to reputation. The actual types of business concerns may vary depending in part on the activities of the organization being evaluated. Application assets are any software programs and associated information data bases that carry out a useful task including transaction systems, database managers, spreadsheets, communications packages, and document processors. Some other examples of application assets are, for example, the software for managing general ledger data, distribution, and product tracking.

The organization must also determine the types of attacks that the organization may be subject to and corresponding countermeasures that may be implemented to avert those attacks (state 105). The set T of attack types, includes but is not limited to, for example, unauthorized access to and use of confidential business information, unauthorized deletion, destruction or modification of data records, and interruption or denial of service. The set M of countermeasures may include, for example, employing a person (such as an account or security administrator to oversee security measures), implementing a technique (such as password protection, event logging, or authentication), or a installing a device (such as a particular secure network configuration). Attack and countermeasure types may also vary depending on the application being evaluated, the type of business concerns, and the organization's corporate and computing architecture.

Consistent with the present invention, information is gathered that describes the application assets and system architecture of the organization, details about daily

operations, and the countermeasures employed at the time of assessment (state 110). In one implementation, this information is obtained by using a questionnaire that is answered by personnel familiar with the organization's operations, although other mechanisms for obtaining the information may be used such as, for example, automated interrogation of computer configurations and networked security services. The questionnaire is tailored to solicit information consistent with the parameters identified above. For example, if corporate training is identified as a countermeasure, then the questionnaire will ask questions such as how often training is performed, what type of training is given, and who delivers the training. One example of a questionnaire consistent with the present invention is shown in Fig. 2.

The identified parameters are used to generate two parameter tables as shown in of Figs. 3A and 3B (state 115). Table 1 of Fig. 3A, for example, shows identified business concerns in the lefthand column and attack types across the top. Each table entry, $\phi_{i,j}$, represents the probability that business concern, c_i, will result from attack t_j. determined by independent security councils of security consulting organizations or from existing data from actual business practice.

Table 2 of Fig. 3B is a vulnerability profile showing the set of countermeasures in the left hand column and attack types across the top. Each table entry, $g_{i,j}$, represents the probability that countermeasure, m_i, will avert attack type, t_j. The probabilities may be determined by independent security councils of security consulting organizations or from existing data from actual business practice.

Consistent with the present invention, one or more rule data bases are constructed for interpreting the information gathered in state 110 (state 120). The rule data bases may be constructed, for example, as rules for use in determining current and recommended countermeasure strength levels. Rule Base A in Fig. 4 is an example of a rule data base consistent with the present invention. Rule Base A reduces the user input on a questionnaire to a numeric value indicating the current countermeasure strength level. In Fig. 4, countermeasures are listed in the lefthand column. The columns marked "Level 1", "Level 2", etc., indicate the various levels of implementation of a countermeasure. Each of the boxes in the body of the table contains logical rules that determine the current level of a countermeasure for a given

application as implemented by the organization. For example, in box 401, if the answer to question 1.1 on the questionnaire is 1.1.1(no), "Policy Awareness" is accorded a Level 1. As shown in box 402, if the answer to question 2.1 is 2.1.2(yes) and the answer to question 2.2 is 2.2.3(item c), then countermeasure "Corporate Security Awareness" is accorded "Level 4."

Another example of a rule data base consistent with the present invention is a rule data base for detecting exception conditions, referred to herein as Rule Base B, an example of which is shown in Fig. 5. Rule Base B may include, for example, rules for including or excluding various operating system services, such as authentication modules or I/O devices. Rule Base B may also include rules for identifying conditions that may require increasing existing countermeasure strengths, such as organization size or connections to insecure networks such as the Internet. Organization size may include number of employees, users, computers, and connections. Rule Base B may also contain rules for recognizing that combinations of certain countermeasures are indicated and for adjusting countermeasure effectiveness accordingly. In general, Rule Base B identifies special conditions that may require special actions, such as an engineering review, legal action, or additional physical security.

After these parameters are determined for the business of the organization, each application asset in the overall system is evaluated independently using states 125-177. For each application asset, processing begins with computation of a maximum loss factor, V, for the current application asset (state 125). For each c_i in the set of C business concerns, there exists a corresponding v_i representing a monetary value of the loss to the organization if loss of the current application asset results in the business concern c_i. The loss estimate includes such factors as cost to restore, recover, or rebuild the lost or damaged application asset or to recover from the side effects caused by compromise of the application asset, such as loss of market share, loss of revenue from crippled manufacturing operations and loss of intellectual property revenue.

To obtain a maximum loss factor, V, the business concern that would result in the greatest loss if this application asset was compromised is identified. The

maximum value v_i for this application asset is submitted to the function f_1 to obtain a maximum loss factor, V. V may be represented mathematically as follows:

$$V = f_1(\max_{i=1..m} v_i)$$

where v_i is the monetary value of the loss of the i^{th} business concern identified for the current application asset and f_1 is a conversion function that returns a value factor depending on the maximum loss corresponding to a business concern. For example, f_1 may be the following function:

$$f_1(v_i) = \begin{cases} 0.8 & v_i < \$5M \\ 1.0 & \$5M < v_i \leq \$10M \\ 1.2 & \$10M < v_i \leq \$50M \\ 1.5 & \$50M < v_i \leq \$100M \\ 2.0 & v_i > \$100M \end{cases}$$

The outputted numeric factor acts to decrease or increase the required effectiveness level based on the application asset's potential recovery cost, replacement loss, and/or other damage created by the attack. Factors consistent with the present invention, such as the factors in the example above, will likely be developed by a panel of security experts and depend on the organization type.

Next, for each of n countermeasures identified in state 105, the method determines current and recommended strength levels. Current strength level is the level of a countermeasure that the organization was employing at the time of assessment. Current strength level of the n^{th} countermeasure, H_n, is determined using Rule Base A compiled in state 120 and described above (state 130). For example, referring again to Fig. 4, for the countermeasure "Policy Awareness" with reference 1.1, there are four possible levels, L1, L2, L4, and L5. As shown in the block under column "L1," if the answer to question 1.1 on the questionnaire is 1.1.1(no), the countermeasure "Policy Awareness" is accorded a level of "1" (block 401). The value

of H_n is therefore 1. In column "L4", for example, if the answer to question 2.1 is 2.1.2(yes) and the answer to question 2.2 is 2.2.3 (b, or the second choice of three), the level of "Policy Awareness" is 4 and $H_n = 4$ (block 402).

Next, the method determines the current effectiveness level of countermeasure n in preventing attacks of all types against each of the business concerns identified for this application asset (state 135). $A_{n,e}$ represents the probability that a particular countermeasure, m_n, will prevent all types of attack for a specific business concern, c_e. For each business concern, $A_{n,e}$ may be computed as follows:

$$A_{n,e} = \sum_{i=1}^{q} \phi_{e,i} \; g_{n,i} \; k^2$$

for each of e business concerns. The quantity $g_{n,i}$ is the probability that employing countermeasure m_n will avert attack t_i as shown in Table 1 in Figure 3A. The quantity $\phi_{e,i}$ is the probability that attack t_e will cause business concern c_i as shown in Table 2 of Figure 3B. The constant k is a constant designed to establish the numerical range of A.

The maximum effectiveness, S_n, of using a particular countermeasure m_n to avert all attack types is determined in state 140. S_n equals the maximum value that results from multiplying each $A_{n,e}$ by the maximum loss factor, V. S_n may be represented mathematically as follows:

$$S_n = \max_{r=1...q}(A_{n,r}V)k$$

P_n is the recommended strength level for the n^{th} countermeasure (state 145). Function f_2 is a conversion function that accepts as input, S_n, the maximum effectiveness of a particular countermeasure, and returns an ordinal value representing a recommended countermeasure strength level. P_n may be represented mathematically as $P_n = f_2(n,S_n)$. The function $f_2(n,S_n)$ results in an value corresponding with a countermeasure strength level for countermeasure n and differs depending on the number of possible strength levels for the n^{th} countermeasure. For example, if countermeasure 12 has two possible strength levels, $f_2(12,S_n)$ will output a value of 1 or 2. If four strength levels are possible for countermeasure 25, $f_2(25,S_n)$ will output a value of 1, 2, 3, or 4.

The current effectiveness level of the current policy, Λ_n, for each countermeasure is determined using a third function, f_3, that uses current strength level, H_n, as input (state 150). Current policy effectiveness may be represented mathematically as follows:

$$\Lambda_n = S_n f_3(n, H_n)$$

In a function f_3 consistent with the present invention, f_3 returns a ordinal value corresponding to the relative effectiveness of the countermeasure strength level such as in the example below.

$$f_3(n, H_n) = \begin{cases} 20 & 1 < H_n < 20 \\ 40 & 21 < H_n < 40 \\ 60 & 41 < H_n < 60 \\ 80 & 61 < H_n < 80 \\ 100 & H_n \geq 80 \end{cases}$$

The actual values chosen for the ranges in f_3 may vary, however, the exemplary ranges used for function f_3 as shown above were determined by independent security councils of leading security-consulting organizations. Furthermore, for ease of formulation, each of the countermeasures in the examples was assumed to have a linear distribution. The function f_3 for each countermeasure may also be adjusted for nonlinearity of the relative effectiveness of the strength levels of the countermeasures depending on the implementation.

Recommended policy effectiveness, Φ_n, for countermeasure m_n is also determined using the third function, f_3, with recommended strength level, P_n, as input (state 155). Recommended policy effectiveness, Φ_n, may be represented mathematically as:

$$\Phi_n = S_n f_3(P_n)$$

Next, an implementation cost N_n is computed using recommended strength level, P_n (state 157). Implementation cost N_n is the estimated cost to implement the n^{th}

countermeasure at level P_n. Countermeasure efficiency Q_n for the n^{th} countermeasure can then be calculated as follows (state 159):

$$Q_n = \frac{\Phi_n}{N_n}$$

where Φ_n and N_n, respectively, are the recommended strength level and implementation cost for the n^{th} countermeasure. Countermeasure efficiency is useful for selecting between countermeasures of approximately the same effectiveness. A higher efficiency will show a greater payback for a given investment.

After states 130 through 160 are completed for each countermeasure in the set, the process continues with state 170. If there are still countermeasures to evaluate, the method continues with state 165 and evaluates the next countermeasure.

Once all the countermeasures have been evaluated, the level of conformance to recommended security policies is calculated (state 170). The level of conformance of the application system at the time of assessment, or application risk, is the difference between current strength level effectiveness and recommended strength level effectiveness of the countermeasures. In an implementation consistent with the present invention, only the positive differences between current and recommended strength levels are considered. By considering only positive differences, the method does not give credit for "overachieving" or, in other words, implementing security procedures that are well above what is considered necessary to be effective. Overachieving can be costly and add unnecessarily to program expenditures.

In the example where only positive differences are considered, the level of conformance is calculated as follows:

$$\Delta = b - \sum \max(\Phi_n - \Lambda_n, 0)$$

$$\text{where} \quad b = \sum_{\Phi_n \geq a} \Phi_n$$

and Λ_n and Φ_n equal the current effectiveness level and recommended effectiveness level for countermeasure M_n, respectively. A high Δ, or conformance value, indicates a secure application system. The conformance value also quantifies the difference

between the current security level policy and security policies established by industry best practices and, indirectly, the amount of the applications vulnerability, or risk. A total amount of risk to the organization may be estimated by computing the weighted average of multiple application conformance values, weighted by the proportional value of each application to the organization's total application systems value.

There exist a number of conditions that may need to be addressed in order to fine tune the selection method. These "exception conditions" are special conditions that need to be addressed with special rules such as those found in Rule Base B determined in state 120 (state 175). Fig. 5 is an example of additional rules consistent with the present invention that may constitute Rule Base B. For example, if any of the processors in the application system serve multiple functions, such as serving both as a file transfer server and a gateway, some of the countermeasures and recommended countermeasures may need to be adjusted. Additionally, some countermeasure strengths may need to be adjusted if the size of the user population exceeds a designated threshold. Organizations with user populations over a threshold, for example, may want to initiate more formal account management procedures such as periodic mandatory password changes, formal procedures for terminated or inactive accounts, or central password administration.

Another example of an exception condition possibly warranting special attention is number and value of transactions processed by the application. If, for example, the application is used to access bank account data or make large payments, the organization may want to employ added security protections such as formalized configuration management, compartmentalizing data, special audit procedures, or requiring a minimum of two people acknowledge changes to the application code. Applications that are operated on network devices that are physically located in multiple geographic locations may also require special attention. Exception conditions may also take into consideration exceptional costs of implementation, such as licensing, training, installation and development costs.

If there are still application assets to evaluate, the process continues with the next application (state 122). If the last application asset has been evaluated, the method outputs a written report (state 180). In addition to other management

information, the reports may contain specifications of both the current and recommended level of countermeasure implementation. For example, Fig. 6 contains an example of written security policies for implementation of each countermeasure. For example, if the n^{th} countermeasure is "2.1 Requirements for Corporate Security Awareness Training" as shown in Fig. 6, and the recommended strength level for the n^{th} countermeasure is $P_n = 3$, then the method may print out an information security policy like "Training requirement identified, but not formal" and accompanying text as shown for level L3 in Fig. 6.

B. Architecture

Fig. 7 is a block diagram that illustrates a computer system 700 upon which embodiments of the invention may be implemented. Computer system 700 includes a bus 702 or other communication mechanism for communicating information, and a processor 704 coupled with bus 702 for processing information. Computer system 700 also includes a memory 706, which can be a random access memory (RAM) or other dynamic storage device, coupled to bus 702 for storing information, such as the parameter tables, rule data bases, and questionnaire, and instructions to be executed by processor 704. Memory 706 also may be used for storing temporary variables or other intermediate information during execution of instructions to be executed by processor 704. Computer system 700 further includes a read only memory (ROM) 708 or other static storage device coupled to bus 702 for storing static information and instructions for processor 704. A storage device 710, such as a magnetic disk or optical disk, is provided and coupled to bus 702 for storing information and instructions.

Computer system 700 may be coupled via bus 702 to a display 712, such as a cathode ray tube (CRT) or liquid crystal display (LCD), for displaying information to a computer user. An input device 714, including alphanumeric and other keys, is coupled to bus 702 for communicating information and command selections to processor 704. Another type of user input device is cursor control 716, such as a mouse, a trackball or cursor direction keys for communicating direction information and command selections to processor 704 and for controlling cursor movement on display 712. This input device typically has two degrees of freedom in two axes, a

first axis (e.g., x) and a second axis (e.g., y), that allows the device to specify positions in a plane.

An embodiment of the present invention uses a computer system 700 for selecting a security model. Consistent with one implementation of the invention, information from the multiple remote resources is provided by computer system 700 in response to processor 704 executing one or more sequences of one or more instructions contained in memory 706. Such instructions may be read into memory 706 from another computer-readable medium, such as storage device 710. Execution of the sequences of instructions contained in memory 706 causes processor 704 to perform the process states described herein. In an alternative implementation, hard-wired circuitry may be used in place of or in combination with software instructions to implement the invention. Thus implementations of the invention are not limited to any specific combination of hardware circuitry and software.

The term "computer-readable medium" as used herein refers to any media that participates in providing instructions to processor 704 for execution. Such a medium may take many forms, including but not limited to, non-volatile media, volatile media, and transmission media. Non-volatile media includes, for example, optical or magnetic disks, such as storage device 710. Volatile media includes dynamic memory, such as memory 706. Transmission media includes coaxial cables, copper wire, and fiber optics, including the wires that comprise bus 702. Transmission media can also take the form of acoustic or light waves, such as those generated during radio-wave and infra-red data communications.

Common forms of computer-readable media include, for example, a floppy disk, a flexible disk, hard disk, magnetic tape, or any other magnetic medium, a CD-ROM, any other optical medium, punch cards, papertape, any other physical medium with patterns of holes, a RAM, PROM, and EPROM, a FLASH-EPROM, any other memory chip or cartridge, a carrier wave as described hereinafter, or any other medium from which a computer can read.

Various forms of computer readable media may be involved in carrying one or more sequences of one or more instructions to processor 704 for execution. For example, the instructions may initially be carried on magnetic disk of a remote

computer. The remote computer can load the instructions into its dynamic memory and send the instructions over a telephone line using a modem. A modem local to computer system 700 can receive the data on the telephone line and use an infra-red transmitter to convert the data to an infra-red signal. An infra-red detector coupled to bus 702 can receive the data carried in the infra-red signal and place the data on bus 702. Bus 702 carries the data to memory 706, from which processor 704 retrieves and executes the instructions. The instructions received by memory 706 may optionally be stored on storage device 710 either before or after execution by processor 704.

Computer system 700 also includes a communication interface 718 coupled to bus 702. Communication interface 718 provides a two-way data communication coupling to a network link 720 that is connected to local network 722. For example, communication interface 718 may be an integrated services digital network (ISDN) card, a cable modem, or a modem to provide a data communication connection to a corresponding type of telephone line. As another example, communication interface 718 may be a local area network (LAN) card provide a data communication connection to a compatible LAN. Wireless links may also be implemented. In any such implementation, communication interface 718 sends and receives electrical, electromagnetic or optical signals that carry digital data streams representing various types of information.

Network link 720 typically provides data communication through one or more networks to other data devices. For example, network link 720 may provide a connection through local network 722 to a host computer 724 and/or to data equipment operated by an Internet Service Provider (ISP) 726. ISP 726 in turn provides data communication services through the Internet 728. Local network 722 and Internet 728 both use electric, electromagnetic, or optical signals that carry digital data streams. The signals through the various networks and the signals on network link 720 and through communication interface 718, which carry the digital data to and from computer system 700, are exemplary forms of carrier waves transporting the information.

Computer system 700 can send messages and receive data, including program code, through the network(s), network link 720 and communication interface 718. In

the Internet example, a server 730 might transmit a requested code for an application program through Internet 728, ISP 726, local network 722 and communication interface 718. In accordance with the present invention, one such downloaded application allows a user to select security countermeasures and countermeasure strength levels, as described herein. The received code may be executed by processor 704 as it is received, and/or stored in storage device 710, or other non-volatile storage for later execution. In this manner, computer system 700 may obtain application code in the form of a carrier wave.

Although computer system 700 is shown in Fig. 7 as being connectable to one server, 730, those skilled in the art will recognize that computer system 700 may establish connections to multiple servers on Internet 728. Additionally, it is possible to implement methods consistent with the principles of the present invention on other device comprising at least a processor, memory, and a display, such as a personal digital assistant.

C. Conclusion

As described in detail above, methods and apparatus consistent with the present invention select a security model based on input data and rules corresponding to the application. The foregoing description of an implementation of the invention has been presented for purposes of illustration and description. For example, the described implementation includes software but the present invention may be implemented as a combination of hardware and software or in hardware alone. The scope of the invention is therefore defined by the claims and their equivalents.

What is claimed is:

1. A method of selecting a security model for an organization operating an application on the organization's computer network, the method comprising:

(a) determining a current strength level for at least one countermeasure based on input data and rules corresponding to the application; and

(b) determining a recommended strength level for the at least one countermeasure based on the input data and security risk data.

2. A method of selecting a security model for an organization operating an application on the organization's computer network, the method comprising:

(a) determining a current strength level for at least one countermeasure based on input data and rules corresponding to the application;

(b) determining a recommended strength level for the at least one countermeasure based on the input data and security risk data; and

(c) determining a security model based on the current strength level and the recommended strength level, the security model including at least one countermeasure and a corresponding strength level.

3. The method of claim 2, further comprising:

modifying the security model based on at least one exception condition.

4. The method of claim 3, wherein modifying the security model includes:

modifying the security model based on at least one or a combination of:

(a) the organization's size;

(b) countermeasure implementation costs;

(c) number of transactions processed by the application;

(d) monetary value of transactions processed by the application;

(e) number of data transfer interfaces between the application and other applications;

(f) configuration of the computer network; and

(g) number of processors in the computer network.

5. The method of claim 2, further comprising:

modifying the security model if the application shares data with another application.

6. The method of claim 2, further comprising:

modifying the security model if the application operates on computer network devices located in more than one geographic location.

7. The method of claim 2, wherein determining a recommended strength level includes:

determining a recommended strength level for the at least one countermeasure based on the input data and the security risk data, wherein the risk data is based on a set of business concerns, a set of attack types, and the at least one countermeasure.

8. The method of claim 2, further comprising:

(d) determining recommended policy effectiveness for the at least one countermeasure based on the recommended strength level and a maximum effectiveness level;

(e) determining current policy effectiveness based on the current strength level and the maximum effectiveness level; and

(f) determining a level of conformance based on the current policy effectiveness and the recommended policy effectiveness.

9. The method of claim 8, wherein determining a level of conformance includes:

determining a risk of attack to the application that results in at least one of a set of business concerns.

10. The method of claim 2, further comprising:

(d) determining an implementation cost for the at least one countermeasure; and

(e) determining countermeasure efficiency based on a maximum effectiveness level and the recommended strength level for the at least one countermeasure.

11. The method of claim 10, further comprising:

(f) selecting a countermeasure of the at least one countermeasures based on the countermeasure efficiency.

12. The method of claim 10, wherein determining an implementation cost includes:

determining an implementation cost for the at least one countermeasure, wherein the implementation cost is based on at least one or a combination of:

(a) cost to train people to use the selected countermeasure;

(b) cost to license the selected countermeasure;

(c) cost to modify the organization's computer network for to use the selected countermeasure; and

(d) cost to modify the application based on the selected countermeasure.

13. The method of claim 2, wherein determining a current strength level comprises:

obtaining responses to a set of questions relating to security procedures at the organization; and

determining a current strength level for the at least one countermeasure based on the responses and rules related to the questions.

14. An apparatus for selecting a security model for an organization operating an application on the organization's computer network, the apparatus comprising:

a memory having program instructions, and

a processor configured to use the program instructions to:

(a) determine a current strength level for at least one countermeasure based on input data and rules corresponding to the application; and

(b) determine a recommended strength level for the at least one countermeasure based on the input data and security risk data.

15. An apparatus for selecting a security model for an organization operating an application on the organization's computer network, the apparatus comprising:

a memory having program instructions, and

a processor configured to use the program instructions to:

(a) determine a current strength level for at least one countermeasure based on input data and rules corresponding to the application;

(b) determine a recommended strength level for the at least one countermeasure based on the input data and security risk data; and

(c) determine a security model based on the current strength level and the recommended strength level, the security model including at least one countermeasure and a corresponding strength level.

16. The apparatus of claim 15, wherein the processor is further configured to use the program instructions to:

modify the security model based on at least one exception condition.

17. The apparatus of claim 16, wherein the program instruction to modify the security model includes the instruction to:

modify the security model based on at least one or a combination of:

(a) the organization's size;

(b) countermeasure implementation costs;

(c) number of transactions processed by the application;

(d) monetary value of transactions processed by the application;

(e) number of data transfer interfaces between the application and other applications;

(f) configuration of the computer network; and

(g) number of processors in the computer network.

18. The apparatus of claim 15, wherein the processor is further configured to use program instructions to:

modify the security model if the application shares data with another application.

19. The apparatus of claim 15, wherein the processor is further configured to use program instructions to:

modify the security model if the application operates on computer network devices located in more than one geographic location.

20. The apparatus of claim 15, wherein the program instruction to determine a recommended strength level includes an instruction to:

determine a recommended strength level for the at least one countermeasure based on the input data and the security risk data, wherein the risk data is based on a set of business concerns, a set of attack types, and the at least one countermeasure.

21. The apparatus of claim 15, wherein the processor is further configured to use program instructions to:

(d) determine recommended policy effectiveness for the at least one countermeasure based on the recommended strength level and a maximum effectiveness level;

(e) determine current policy effectiveness based on the current strength level and the maximum effectiveness level; and

(f) determine a level of conformance based on the current policy effectiveness and the recommended policy effectiveness.

22. The apparatus of claim 21, wherein the instruction to determine a level of conformance includes an instruction to:

determining a risk of attack to the application that results in at least one of a set of business concerns..

23. The apparatus of claim 15, wherein the processor is further configured to use the program instruction to:

(d) determine an implementation cost for the at least one countermeasure; and

(e) determine countermeasure efficiency based on a maximum effectiveness level and the recommended strength level for the at least one countermeasure.

24. The apparatus of claim 23, wherein the processor is further configured to use the program instruction to:

(f) select a countermeasure of the at least one countermeasures based on the countermeasure efficiency.

25. The apparatus of claim 23, wherein the instruction to determine an implementation cost includes the instruction to:

determine an implementation cost for the at least one countermeasure, wherein the implementation cost is based on at least one or a combination of:

(a) cost to train people to use the selected countermeasure;

(b) cost to license the selected countermeasure;

(c) cost to modify the organization's computer network for to use the selected countermeasure; and

(d) cost to modify the application based on the selected countermeasure.

26. The apparatus of claim 15, wherein the instruction to determine a current strength level includes the instruction to:

obtain responses to a set of questions relating to security procedures at the organization; and

determine a current strength level for the at least one countermeasure based on the responses and rules related to the questions.

27. A computer-readable medium containing instructions for controlling a computer system to perform a method, the computer system having a group of data structures reflecting a logical structure of a data source, the method comprising:

(a) determining a current strength level for at least one countermeasure based on input data and rules corresponding to the application; and

(b) determining a recommended strength level for the at least one countermeasure based on the input data and security risk data.

28. A computer-readable medium containing instructions for controlling a computer system to perform a method, the computer system having a group of data structures reflecting a logical structure of a data source, the method comprising:

(a) determining a current strength level for at least one countermeasure based on input data and rules corresponding to the application;

(b) determining a recommended strength level for the at least one countermeasure based on the input data and security risk data; and

(c) determining a security model based on the current strength level and the recommended strength level, the security model including at least one countermeasure and a corresponding strength level.

29. The computer-readable medium of claim 28, further including:

modifying security model based on at least one exception condition.

30. The computer-readable medium of claim 29, wherein modifying the security model includes:

modifying the security model based on at least one or a combination of:

(a) the organization's size;

(b) countermeasure implementation costs;

(c) number of transactions processed by the application;

(d) monetary value of transactions processed by the application;

(e) number of data transfer interfaces between the application and other applications;

(f) configuration of the computer network; and

(g) number of processors in the computer network.

31. The computer-readable medium of claim 28, further including:

modifying the security model if the application shares data with another application.

32. The computer-readable medium of claim 28, further including:

modifying the security model if the application operates on computer network devices located in more than one geographic location.

33. The computer-readable medium of claim 28, wherein determining a recommended strength level for the at least one countermeasure based on the input data and the security risk data includes:

determining a recommended strength level for the at least one countermeasure based on the input data and security risk data, wherein the risk data is based on a set of business concerns, a set of attack types, and the at least one countermeasure.

34. The computer-readable medium of claim 28, further comprising:

(d) determining recommended policy effectiveness for the at least one countermeasure based on the recommended strength level and a maximum effectiveness level;

(e) determining current policy effectiveness based on the current strength level and the maximum effectiveness level; and

(f) determining a level of conformance based on the current policy effectiveness and the recommended policy effectiveness.

35. The computer-readable medium of claim 28, wherein determining a level of conformance includes:

determining a risk of attack to the application that results in at least one of a set of business concerns.

36. The computer-readable medium of claim 28, further comprising:

(d) determining an implementation cost for the at least one countermeasure; and

(e) determining countermeasure efficiency based on a maximum effectiveness level and the recommended strength level for the at least one countermeasure.

37. The computer-readable medium of claim 35, further comprising:

(f) selecting a countermeasure of the at least one countermeasure based on the recommended efficiency level.

38. The computer-readable medium of claim 35, wherein determining an implementation cost includes:

determining an implementation cost for the at least one countermeasure, wherein the implementation cost is based on at least one or a combination of:

(a) cost to train people to use the selected countermeasure;

(b) cost to license the selected countermeasure;

(c) cost to modify the organization's computer network for to use the selected countermeasure; and

(d) cost to modify the application based on the selected countermeasure.

39. The computer-readable medium of claim 28, wherein determining a current strength level includes:

obtaining responses to a set of questions relating to security procedures at the organization; and

determining a current strength level for the at least one countermeasure based on the responses and a rules related to the questions.

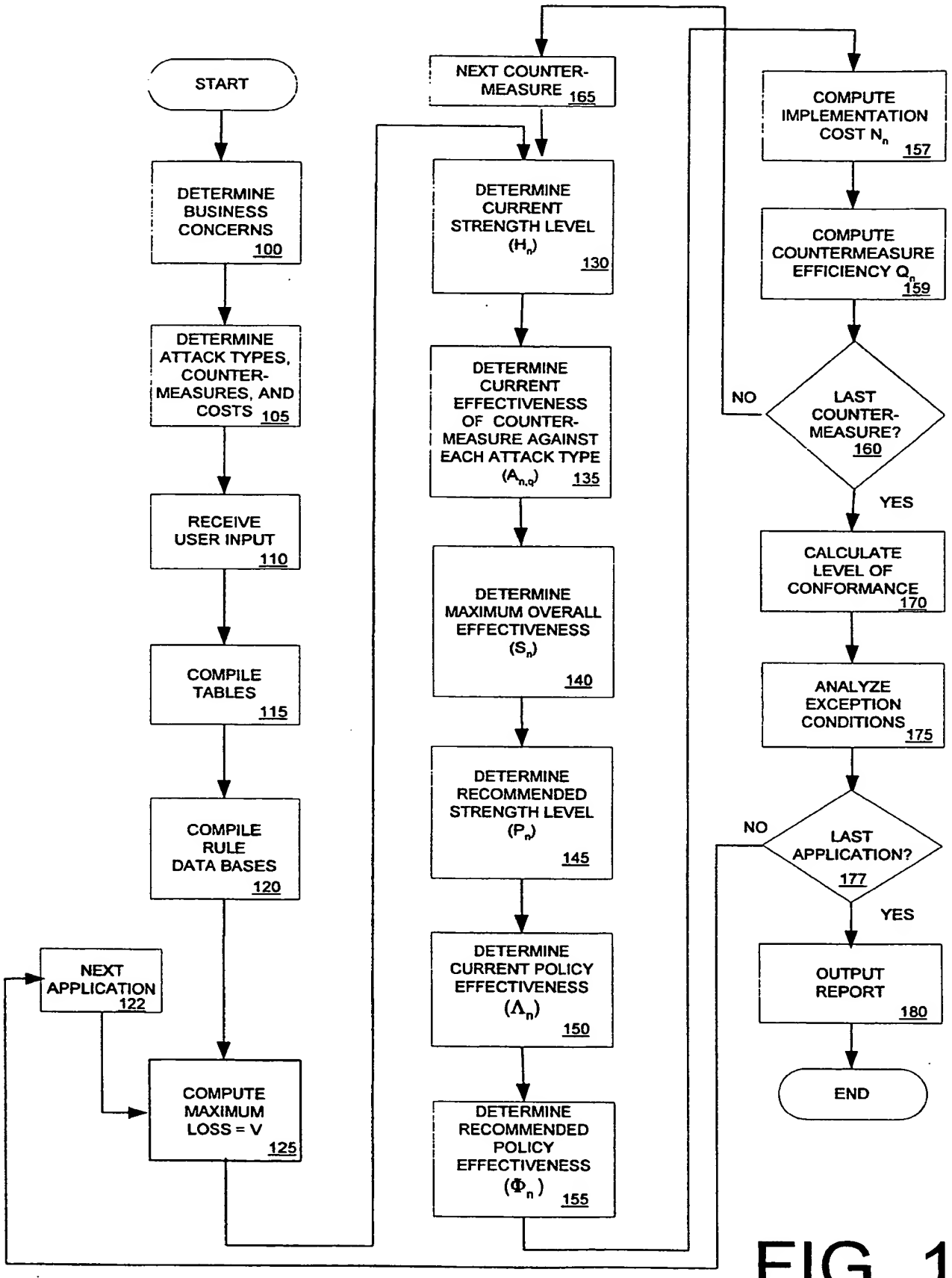


FIG. 1

POLICY 1.0
1. Is there a security policy for this application system?
(.1) No (.2) Yes

2. Describe the your knowledge level of the Application System security policy?
(a) Informal policy exists.
(b) A policy has been distributed.
(c) I have personal knowledge of the policy and procedures.

4. Is there a process in place for security policy compliance?
(.1) No (.2) Yes

5. Are exceptions to policy allowed, if so how are they submitted?
(.1) No (.2) Yes
Explain the exception: _____
TRAINING 2.0
1. Are you aware of any corporate security training programs?
(.1) No (.2) Yes

2. Which statement best describes the corporate security training program?
(a) None
(b) Training is informal.
(c) Training available, but not required
(d) Training is defined courses are available and required
Please list any security training that you are aware of: _____

5. Have you received any unique Application Systems security training?
(.1) No (.2) Yes

3a. Which statement describes any Application System unique security training that is available
(a) None
(b) Training is informal
(c) Training requirement identified but not formal
(d) Training courses identified and mandatory
If yes please describe._____

4. Are security training compliance measurements and monitoring procedures in place?
(a) Yes
(b) No
(c) Don't Know.
5. Training compliance is monitored by:
(a) 1st level supervisor
(b) Department Manager
(c) Training department.

FIG. 2

TABLE 1: Attack Signatures

Attack Types, T_j

Business Concerns C_i

	Disclosure	Modification	Interruption/ Denial of Svc	Deletion/ Destruction
Embarassment/ Reputation	0.6	0.8	0.4	0.4
Extortion	1	0.6	0.8	0.8
Fraud/ Embezzlement	0.8	1	0	0.4
Loss of market share/ increased competition	1	0.8	0	0

FIG. 3A

TABLE 2: Vulnerability Profile

Attack Types, T_j

Counter-measures M_i

	Disclosure	Modification	Interruption/ Denial of Svc	Deletion/ Destruction
Policy Awareness	0.6	0.6	0.4	0.4
Policy Compliance	0.8	0.8	0.4	0.6
Corporate Security Awareness	0.6	0.6	0.4	0.4
Unique Training	0.6	0.6	0.4	0.4
Account Revocation				

FIG. 3B

Reference	M(n) Countermeasure	I(n) Level 1	Level 2	Level 3	Level 4	Level 5
1.1	Policy Awareness	1.1.1 **401**	1.1.2 & 1.2.1		1.1.2 & 1.2.2	1.1.2 & 1.2.3
1.2	Policy Compliance	1.3.1		1.3.2 & 1.4.2		1.3.2 & 1.4.1
2.1	Corporate Security Awareness	2.1.1 or 2.2.1	2.1.2 & 2.2.2		2.1.2 & 2.2.3 **402**	2.1.2 & 2.2.4
2.2	Unique Training	2.3.1 or 2.3a.1	2.3.2 & 2.3a.2		2.3.2 & 2.3a.3	2.3.2 & 2.3a.4
2.3	Training Compliance*	2.3.1 & (2.4.1 or 2.4.3)	2.3.2 & 2.4.3		2.3.2 & 2.4.2	2.3.2 & 2.4.2 & 2.5.x
3.1	Authorization End User	(3.1.1 & 3.2.1) or 3.6.3	(3.1.1 & 3.2.2) & 1 of, 3.3a.2, 3.4a.2, 3.5a.2, (3.7.1 or 3.7.2 or 3.7.3)	(3.1.1 & 3.2.2) & 2 of, 3.3a.2, 3.4a.2, 3.5a.2, (3.7.1 or 3.7.2 or 3.7.3)	(3.1.1 & 3.2.2) & 4 of, 3.3a.2, 3.4a.2, 3.5a.2, (3.7.1 or 3.7.2 or 3.7.3)	(3.1.1 & 3.2.2) & 3.7.4 & 3 of, 3.3a.2, 3.4a.2, 3.5a.2

FIG. 4

1) Is the number of users is greater than 150? If so, then implement more rigid account management procedures including:

- Formal procedures with revocation/modification of terminated or inactive accounts.
- Passwords centrally assigned and monitored, with quarterly password cracking in place.
- Each user has unique password with 90-day mandatory password changing
- All new passwords are screened for suitability prior to system acceptance

2) Is the application system transaction value greater than $5 million per quarter OR
Is the application system a Data Base of Record? If so, implement formal configuration management procedures with quality assurance including:

- Two- person rule for all code-level alterations
- Quality assurance testing of all code prior to acceptance on production system
- Compartmentalize data within Intranet using firewall and/or other solutions

Etc.

FIG. 5

INFORMATION SECURITY POLICIES

2.0 Training

This policy addresses the requirements for identifying training needs specific to an application system, and the general need for corporate security awareness training. The policy also covers compliance with the delivery of training to the appropriate personnel. The policy applies to all company personnel who manage, administer and use the application system. If the application system is also used by non-employees, it is the responsibility of the system owner to ensure that any needed training requirements are identified for them, and that appropriate non-employees have access to and receive the necessary training to operate the application system properly and securely.

2.1 Requirements For Corporate Security Awareness Training In The Operation Of An Application System.

L1 – *No specific training identified.*

L2 – Use L3.

L3 – *Training requirement identified, but not formal.* The application system owner may determine which personnel, if any, must attend corporate security awareness training classes. Other personnel may be given a security briefing, written corporate security policies, a corporate security awareness video, or the policy summary for the application system.

L4 – Use L5.

L5 – *Training identified and courses available.* The application system owner must indicate which personnel are required to take standard corporate security awareness classes. If the system owner determines that the standard courses are not sufficient for the sensitivity of the application system, arrangements must be made with the corporate training department to produce and offer courses which do meet the need. The training must include procedures for reporting suspected security incidents and for escalating serious security events to appropriate managers.

2.2 Requirements For Unique Security Training For The Successful Operation Of An Application System.

L1 – *No specific training identified.*

L2 – Use L3.

L3 – *Training requirement identified, but not formal.* The application system owner has determined there are security needs specific to the application system which require special training. The application system owner, or a designated representative, is responsible for providing the special training by means of briefings, demonstrations, or written materials.

L4 – Use L5.

L5 – *Training identified and courses available.* The application system owner has determined there are security needs specific to the application system which require special training. The application system owner is responsible for ensuring that the corporate training department has the necessary input and resources to produce the required courses, and that the courses are available to personnel in time to meet production schedules.

FIG. 6

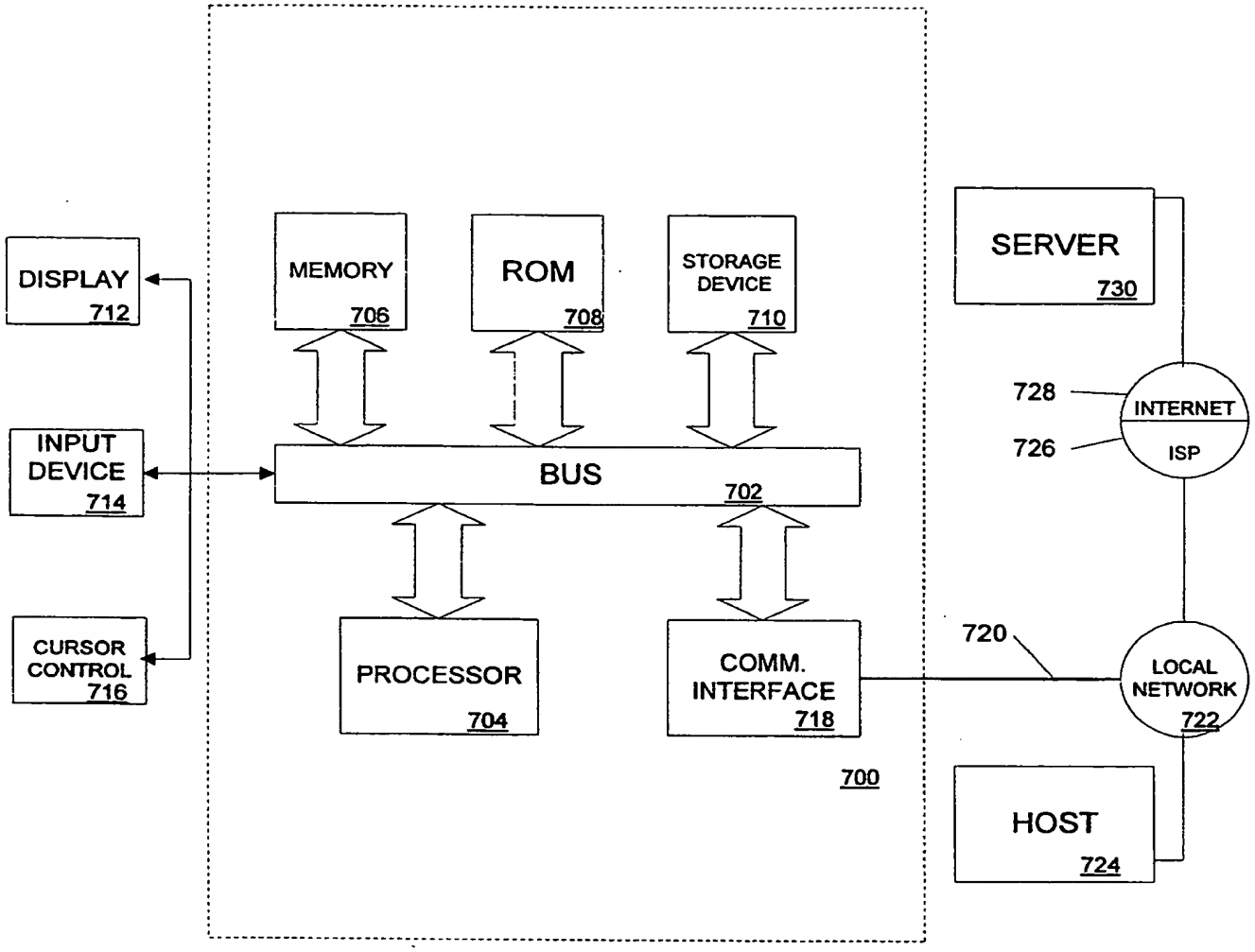


FIG. 7

INTERNATIONAL SEARCH REPORT

Inte onal Application No
PCT/US 99/17575

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category '	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	L. LABUSCHAGNE AND J. H. P. ELOFF: "The use of Real-Time risk analysis to enable dynamic activation of countermeasures" COMPUTER & SECURITY (ELSEVIER), vol. 17, no. 4, 1998, pages 347-357, XP004129259 the whole document ---	1,14,15, 27,28
A	US 5 533 123 A (G. FORCE ET AL.) 2 July 1996 (1996-07-02) column 1, line 1 -column 4, line 63 column 23, line 15 -column 27, line 51; tables I,II -----	1,14,15, 27,28

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

' Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 December 1999	22/12/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040. Tx. 31 651 epo nl. Fax: (+31-70) 340-3016	Soler, J

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

nformation on patent family members

Inte onal Application No
PCT/US 99/17575

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5533123 A	02-07-1996	EP 0715733 A	12-06-1996
		WO 9600953 A	11-01-1996

Form PCT/ISA/210 (patent family annex) (July 1992)